



National Critical Information Infrastructure Protection Centre

CVE Report

01-15 Sep 2017

Vol. 04 No.15

Vulnerability Type(s)	Publish Date	CVSS	Description CVE ID	Patch	NCIIPC ID
Application (A)					
Apache					
Hadoop					
Gain Information	2017-09-05	5	The YARN NodeManager in Apache Hadoop 2.6.x before 2.6.5 and 2.7.x before 2.7.3 can leak the password for credential store provider used by the NodeManager to YARN Applications. CVE-2016-3086	NA	A-APA-HADOO-140817/1
Askbot					
Askbot					
XSS	2017-09-07	4.3	Cross-site scripting (XSS) vulnerability in askbot 0.7.51-4.el6.noarch. CVE-2015-3169	https://bugzilla.redhat.com/show_bug.cgi?id=1221616	A-ASK-ASKBO-140817/2
Aspl					
Libaxl					
DoS Execute Code Overflow Memory Corruption	2017-09-06	6.8	Heap-based buffer overflow in libaxl 0.6.9 allows attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted XML document. CVE-2015-3450	NA	A-ASP-LIBAX-140817/3
Beaker-project					
Beaker					
NA	2017-09-06	4	The admin pages for power types and key types in Beaker before 20.1 do not have any access controls, which allows remote authenticated users to modify power types and key types via navigating to \$BEAKER/powertypes and	https://bugzilla.redhat.com/show_bug.cgi?id=1215034	A-BEA-BEAKE-140817/4

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			\$BEAKER/keytypes respectively. CVE-2015-3163		
XSS	2017-09-06	3.5	Cross-site scripting (XSS) vulnerability in the edit comment dialog in bkr/server/widgets.py in Beaker 20.1 allows remote authenticated users to inject arbitrary web script or HTML via writing a crafted comment on an acked or nacked cancelled job. CVE-2015-3162	https://beaker-project.org/docs/whats-new/release-20.html#bug-fixes	A-BEA-BEAKE-140817/5
XSS	2017-09-06	3.5	The search bar code in bkr/server/widgets.py in Beaker before 20.1 does not escape </script> tags in string literals when producing JSON. CVE-2015-3161	https://bugzilla.redhat.com/show_bug.cgi?id=1215024	A-BEA-BEAKE-140817/6
Gain Information	2017-09-06	4	XML external entity (XXE) vulnerability in bkr/server/jobs.py in Beaker before 20.1 allows remote authenticated users to obtain sensitive information via submitting job XML to the server containing entity references which reference files from the Beaker server's file system. CVE-2015-3160	https://bugzilla.redhat.com/attachment.cgi?id=1020003	A-BEA-BEAKE-140817/7

Bento4

Bento4

DoS	2017-09-06	4.3	The AP4_AvccAtom::InspectFields function in Core/AvccAtom.cpp in Bento4 mp4dump before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application	NA	A-BEN-BENTO-140817/8
-----	------------	-----	---	----	----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			crash) via a crafted mp4 file. CVE-2017-12476		
DoS	2017-09-06	4.3	The AP4_Processor::Process function in Core/Ap4Processor.cpp in Bento4 mp4encrypt before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE-2017-12475	NA	A-BEN-BENTO-140817/9
DoS	2017-09-06	4.3	The AP4_AtomSampleTable::GetSample function in Core/Ap4AtomSampleTable.cpp in Bento4 mp42ts before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE-2017-12474	NA	A-BEN-BENTO-140817/10
DoS	2017-09-06	4.3	The AP4_AvccAtom::InspectFields function in Core/Ap4AvccAtom.cpp in Bento4 mp4dump before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE-2017-12476	NA	A-BEN-BENTO-140817/11
Bento4					
DoS	2017-09-06	4.3	The AP4_Processor::Process function in Core/Ap4Processor.cpp in Bento4 mp4encrypt before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE-2017-12475	NA	A-BEN-BENTO-140817/12

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

DoS	2017-09-06	4.3	The AP4_AtomSampleTable::GetSample function in Core/Ap4AtomSampleTable.cpp in Bento4 mp42ts before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE-2017-12474	NA	A-BEN-BENTO-140817/13
-----	------------	-----	---	----	-----------------------

Community Events Project

Community Events

Sql	2017-09-07	7.5	SQL injection vulnerability in WordPress Community Events plugin before 1.4. CVE-2015-3313	https://wordpress.org/plugins/community-events/#developers	A-COM-COMMU-140817/14
-----	------------	-----	--	---	-----------------------

Concrete5

Concrete5

Sql	2017-09-07	7.5	SQL injection vulnerability in Concrete5 5.7.3.1. CVE-2015-4724	http://hackerone.com/reports/59664	A-CON-CONCR-140817/15
XSS	2017-09-07	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Concrete5 5.7.3.1. CVE-2015-4721	http://hackerone.com/reports/59661	A-CON-CONCR-140817/16

Dreambox

Opendreambox

Execute Code	2017-09-04	10	enigma2-plugins/blob/master/webadmin/src/WebChilds/Script.py in the webadmin plugin for opendreambox 2.0.0 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the command parameter to the /script URI. CVE-2017-14135	https://theinfosec.com/2017/07/05/from-shodan-to-rce-opendreambox-2-0-0-code-execution/	A-DRE-OPEND-140817/17
--------------	------------	----	--	---	-----------------------

Embedthis

Goahead

NA	2017-09-05	5	GoAhead 3.4.0 through 3.6.5 has a NULL Pointer	https://github.com/shadow4u/goahead	A-EMB-GOAHE-
----	------------	---	--	---	--------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			Dereference in the websDecodeUrl function in http.c, leading to a crash for a "POST / HTTP/1.1" request. CVE-2017-14149	aheaddebug/blob/master/README.md	140817/18
--	--	--	--	----------------------------------	-----------

Epicor

Crs Retail Store

Execute Code	2017-09-06	7.2	The help window in Epicor CRS Retail Store before 3.2.03.01.008 allows local users to execute arbitrary code by injecting Javascript into the window source to create a button that spawns a command shell. CVE-2015-2210	NA	A-EPI-CRS R-140817/19
--------------	------------	-----	---	----	-----------------------

Eyesofnetwork

Eonweb

Execute Code	2017-09-03	6.5	In the EyesOfNetwork web interface (aka eonweb) 5.1-0, module\tool_all\tools\snmpwalk.php does not properly restrict popen calls, which allows remote attackers to execute arbitrary commands via shell metacharacters in a parameter. CVE-2017-14119	http://kk.whitecell-club.org/index.php/archives/220/	A-EYE-EONWE-140817/20
Execute Code	2017-09-03	6.5	In the EyesOfNetwork web interface (aka eonweb) 5.1-0, module\tool_all\tools\interface.php does not properly restrict exec calls, which allows remote attackers to execute arbitrary commands via shell metacharacters in the host_list parameter to module/tool_all/select_tool.php. CVE-2017-14118	http://kk.whitecell-club.org/index.php/archives/220/	A-EYE-EONWE-140817/21

Finecms Project

Finecms

XSS	2017-09-07	4.3	The call_msg function in	http://bendawa	A-FIN-FINEC-
-----	------------	-----	--------------------------	---	--------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			controllers/Form.php in dayrui FineCms 5.0.11 might have XSS related to the Referer HTTP header with Internet Explorer. CVE-2017-14195	ng.site/article/finecms-V5.0.11-multi-vulnerability	140817/22
XSS	2017-09-07	4.3	The out function in controllers/member/Login.php in dayrui FineCms 5.0.11 has XSS related to the Referer HTTP header with Internet Explorer. CVE-2017-14194	http://bendawang.site/article/finecms-V5.0.11-multi-vulnerability	A-FIN-FINEC-140817/23
XSS	2017-09-07	4.3	The oauth function in controllers/member/api.php in dayrui FineCms 5.0.11 has XSS related to the Referer HTTP header with Internet Explorer. CVE-2017-14193	http://bendawang.site/article/finecms-V5.0.11-multi-vulnerability	A-FIN-FINEC-140817/24
XSS	2017-09-07	4.3	The checktitle function in controllers/member/api.php in dayrui FineCms 5.0.11 has XSS related to the module field. CVE-2017-14192	http://bendawang.site/article/finecms-V5.0.11-multi-vulnerability	A-FIN-FINEC-140817/25

Ffmpeg

Ffmpeg

NA	2017-09-07	7.1	In libavformat/nsvdec.c in FFmpeg 3.3.3, a DoS in nsv_parse_NSVf_header() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted NSV file, which claims a large "table_entries_used" field in the header but does not contain sufficient backing data, is provided, the loop over 'table_entries_used' would consume huge CPU resources, since there is no EOF check inside the loop. CVE-2017-14171	https://github.com/FFmpeg/FFmpeg/commit/c24bcb553650b91e9eff15ef6e54ca73de2453b7	A-FFM-FFMPE-140817/26
----	------------	-----	--	--	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

NA	2017-09-07	7.1	In libavformat/mxfdec.c in FFmpeg 3.3.3, a DoS in mxf_read_index_entry_array() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted MXF file, which claims a large "nb_index_entries" field in the header but does not contain sufficient backing data, is provided, the loop would consume huge CPU resources, since there is no EOF check inside the loop. Moreover, this big loop can be invoked multiple times if there is more than one applicable data segment in the crafted MXF file. CVE-2017-14170	https://github.com/FFmpeg/FFmpeg/commit/900f39692ca0337a98a7cf047e4e2611071810c2	A-FFM-FFMPE-140817/27
Bypass	2017-09-07	6.8	In the mxf_read_primer_pack function in libavformat/mxfdec.c in FFmpeg 3.3.3, an integer signedness error might occur when a crafted file, which claims a large "item_num" field such as 0xffffffff, is provided. As a result, the variable "item_num" turns negative, bypassing the check for a large value. CVE-2017-14169	https://github.com/FFmpeg/FFmpeg/commit/9d00fb9d70ee8c0cc7002b89318c5be00f1bbdad	A-FFM-FFMPE-140817/28

Fujixerox

Contentsbridge Utility

Gain Privileges	2017-09-01	9.3	Untrusted search path vulnerability in Installer for ContentsBridge Utility for Windows 7.4.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	http://www.fujixerox.co.jp/company/news/notice/2017/0831_rectification_work.html	A-FUJ-CONTE-140817/29
-----------------	------------	-----	---	---	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			CVE-2017-10851		
Docuworks					
Gain Privileges	2017-09-01	9.3	Untrusted search path vulnerability in Self-extracting document generated by DocuWorks 8.0.7 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. CVE-2017-10849	http://www.fujixerox.co.jp/company/news/notice/2017/0831_rectification_work.html	A-FUJ-DOCUW-140817/30
Docuworks;Docuworks Viewer Light					
Gain Privileges	2017-09-01	9.3	Untrusted search path vulnerability in Installers for DocuWorks 8.0.7 and earlier and DocuWorks Viewer Light published in Jul 2017 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. CVE-2017-10848	http://www.fujixerox.co.jp/company/news/notice/2017/0831_rectification_work.html	A-FUJ-DOCUW-140817/31
Froxlор					
Froxlор					
Gain Information	2017-09-06	5	Froxlор before 0.9.33.2 with the default configuration/setup might allow remote attackers to obtain the database password by reading /logs/sql-error.log. CVE-2015-5959	https://github.com/Froxlор/Froxlор/commit/8558533a9148a2a0302c9c177abff8e4e4075b92	A-FRO-FROXL-140817/32
Graphicsmagick					
Graphicsmagick					
DoS Overflow	2017-09-06	4.3	The ReadSUNImage function in coders/sun.c in GraphicsMagick 1.3.26 has an issue where memory allocation is excessive because it depends only on a length field in a header. This may lead to remote denial of service in the MagickMalloc function in	NA	A-GRA-GRAPH-140817/33

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			magick/memory.c CVE-2017-14165		
NA	2017-09-01	6.8	The ReadJNGImage and ReadOneJNGImage functions in coders/png.c in GraphicsMagick 1.3.26 do not properly manage image pointers after certain error conditions, which allows remote attackers to conduct use-after-free attacks via a crafted file, related to a ReadMNGImage out-of-order CloseBlob call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11403. CVE-2017-14103	NA	A-GRA-GRAPH-140817/34
NA	2017-09-01	6.8	The ReadJNGImage and ReadOneJNGImage functions in coders/png.c in GraphicsMagick 1.3.26 do not properly manage image pointers after certain error conditions, which allows remote attackers to conduct use-after-free attacks via a crafted file, related to a ReadMNGImage out-of-order CloseBlob call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11403. CVE-2017-14103	NA	A-GRA-GRAPH-140817/35

GNU

Binutils

DoS Overflow	2017-09-04	4.3	The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=2a143b99fc4a5094a9cf128f3184d8e6818c8229	A-GNU-BINUT-140817/36
--------------	------------	-----	---	---	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			and application crash) via a crafted ELF file. CVE-2017-14130		
DoS Overflow	2017-09-04	4.3	The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF file. CVE-2017-14129	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=e4f2723003859dc6b33ca0dadbc4a7659ebf1643	A-GNU-BINUT-140817/37
DoS Overflow	2017-09-04	4.3	The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file. CVE-2017-14128	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=7e8b60085eb3e6f2c41bc0c00c0d759fa7f72780	A-GNU-BINUT-140817/38

Gnome

Evince

Execute Code	2017-09-05	6.8	backend/comics/comics-document.c (aka the comic book backend) in GNOME Evince before 3.24.1 allows remote attackers to execute arbitrary commands via a .cbt file that is a TAR archive containing a filename beginning with a "--" command-line option substring, as demonstrated by a --checkpoint-action=exec=bash at the beginning of the filename. CVE-2017-100083	NA	A-GNO-EVINC-140817/39
--------------	------------	-----	---	----	-----------------------

Gedit

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

DoS	2017-09-05	7.1	libgedit.a in GNOME gedit through 3.22.1 allows remote attackers to cause a denial of service (CPU consumption) via a file that begins with many '\0' characters. CVE-2017-14108	NA	A-GNO-GEDIT-140817/40
DoS	2017-09-05	7.1	libgedit.a in GNOME gedit through 3.22.1 allows remote attackers to cause a denial of service (CPU consumption) via a file that begins with many '\0' characters. CVE-2017-14108	NA	A-GNO-GEDIT-140817/41

Gdk-pixbuf

Execute Code Overflow	2017-09-05	6.8	An exploitable integer overflow vulnerability exists in the tiff_image_parse functionality of Gdk-Pixbuf 2.36.6 when compiled with Clang. A specially crafted tiff file can cause a heap-overflow resulting in remote code execution. An attacker can send a file or a URL to trigger this vulnerability. CVE-2017-2870	NA	A-GNO-GDK-P-140817/42
Execute Code Overflow	2017-09-05	6.8	An exploitable heap overflow vulnerability exists in the gdk_pixbuf_jpeg_image_load_increment functionality of Gdk-Pixbuf 2.36.6. A specially crafted jpeg file can cause a heap overflow resulting in remote code execution. An attacker can send a file or url to trigger this vulnerability. CVE-2017-2862	NA	A-GNO-GDK-P-140817/43

Helpdezk

Helpdezk

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

Execute Code	2017-09-05	6.5	HelpDEZk 1.1.1 allows remote authenticated users to execute arbitrary PHP code by uploading a .php attachment and then requesting it in the helpdez\app\uploads\helpdez\attachments\ directory. CVE-2017-14146	https://github.com/M4ple/vulnerability/blob/master/helpdez_file_upload/helpdez_k_file_upload.md	A-HEL-HELPD-140817/44
Sql	2017-09-05	7.5	HelpDEZk 1.1.1 has SQL Injection in app\modules\admin\controllers\loginController.php via the admin/login/getWarningInfo/id/ PATH_INFO, related to the selectWarning function. CVE-2017-14145	https://github.com/M4ple/vulnerability/blob/master/helpdez_sql/helpdez_sql_injection.md	A-HEL-HELPD-140817/45
Honda					
<i>Moto Linc</i>					
NA	2017-09-06	4.3	Honda Moto LINC 1.6.1 does not verify SSL certificates. CVE-2015-2943	NA	A-HON-MOTO-140817/46
Imagemagick					
<i>Imagemagick</i>					
NA	2017-09-07	7.1	In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "length" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop. CVE-2017-14174	https://github.com/ImageMagick/ImageMagick/commit/04a567494786d5bb50894fc8bb8fea0cf496bea8	A-IMA-IMAGE-140817/47
Overflow	2017-09-07	4.3	In the function	https://github.com	A-IMA-IMAGE-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			<p>ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation</p> <p>"GetQuantumRange(depth)+1" when "depth" is large, producing a smaller value than expected. As a result, an infinite loop would occur for a crafted TXT file that claims a very large "max_value" value.</p> <p>CVE-2017-14173</p>	m/ImageMagick /ImageMagick/issues/713	140817/48
NA	2017-09-07	7.1	<p>In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "extent" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.</p> <p>CVE-2017-14172</p>	https://github.com/ImageMagick/ImageMagick/issues/715	A-IMA-IMAGE-140817/49
Overflow	2017-09-04	6.8	<p>ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMSLImage in coders/msl.c.</p> <p>CVE-2017-14139</p>	https://github.com/ImageMagick/ImageMagick/issues/578	A-IMA-IMAGE-140817/50
Overflow	2017-09-04	7.5	<p>ImageMagick 7.0.6-5 has a memory leak vulnerability in ReadWEBPImage in coders/webp.c because memory is not freed in certain error cases, as demonstrated by VP8 errors.</p> <p>CVE-2017-14138</p>	https://github.com/ImageMagick/ImageMagick/issues/639	A-IMA-IMAGE-140817/51
Overflow	2017-09-04	7.5	<p>ReadWEBPImage in coders/webp.c in</p>	https://github.com/ImageMagick	A-IMA-IMAGE-140817/52

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
<p>Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable</p>										

			ImageMagick 7.0.6-5 has an issue where memory allocation is excessive because it depends only on a length field in a header. CVE-2017-14137	/ImageMagick/issues/641	
DoS	2017-09-01	7.1	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file. CVE-2017-12693	https://github.com/ImageMagick/ImageMagick/issues/652	A-IMA-IMAGE-140817/53
DoS	2017-09-01	7.1	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file. CVE-2017-12692	https://github.com/ImageMagick/ImageMagick/issues/653	A-IMA-IMAGE-140817/54
DoS	2017-09-01	7.1	The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file. CVE-2017-12691	https://github.com/ImageMagick/ImageMagick/issues/656	A-IMA-IMAGE-140817/55
DoS	2017-09-01	7.1	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file. CVE-2017-12693	https://github.com/ImageMagick/ImageMagick/issues/652	A-IMA-IMAGE-140817/56
DoS	2017-09-01	7.1	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file. CVE-2017-12692	https://github.com/ImageMagick/ImageMagick/issues/653	A-IMA-IMAGE-140817/57
DoS	2017-09-01	7.1	The ReadOneLayer function in coders/xcf.c in	https://github.com/ImageMagick	A-IMA-IMAGE-140817/58

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file. CVE-2017-12691	/ImageMagick/issues/656	
IBM					
Qradar Network Security					
NA	2017-09-05	5	IBM QRadar Network Security 5.4 supports interaction between multiple actors and allows those actors to negotiate which algorithm should be used as a protection mechanism such as encryption or authentication, but it does not select the strongest algorithm that is available to both parties. IBM X-Force ID: 128689. CVE-2017-1491	http://www.ibm.com/support/docview.wss?uid=swg22007535	A-IBM-QRADA-140817/59
NA	2017-09-05	5.5	IBM QRadar Network Security 5.4 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 128377. CVE-2017-1458	http://www.ibm.com/support/docview.wss?uid=swg22007551	A-IBM-QRADA-140817/60
XSS	2017-09-05	4.3	IBM QRadar Network Security 5.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128376. CVE-2017-1457	http://www.ibm.com/support/docview.wss?uid=swg22007550	A-IBM-QRADA-140817/61

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			function in libjasper/base/jas_image.c. CVE-2017-14132		
Ldapauth-fork Project					
Ldapauth-fork					
NA	2017-09-06	5	ldapauth-fork before 2.3.3 allows remote attackers to perform LDAP injection attacks via a crafted username. CVE-2015-7294	https://github.com/vesse/node-ldapauth-fork/issues/21	A-LDA-LDAPA-140817/66
Lexmark					
Scan To Network					
Gain Information	2017-09-07	5	Lexmark Scan To Network (SNF) 3.2.9 and earlier stores network configuration credentials in plaintext and transmits them in requests, which allows remote attackers to obtain sensitive information via requests to (1) cgi-bin/direct/printer/prtappauth/apps/snfDestServlet or (2) cgi-bin/direct/printer/prtappauth/apps/ImportExportServlet. CVE-2017-13771	NA	A-LEX-SCAN - 140817/67
Perceptive Document Filters					
Execute Code Overflow	2017-09-05	6.8	An exploitable code execution vulnerability exists in the image rendering functionality of Lexmark Perceptive Document Filters 11.3.0.2400. A specifically crafted PDF can cause a function call on a corrupted DCTStream to occur, resulting in user controlled data being written to the stack. A maliciously crafted PDF file can be used to trigger this vulnerability. CVE-2017-2822	NA	A-LEX-PERCE-140817/68

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

Execute Code	2017-09-05	6.8	An exploitable use-after-free exists in the PDF parsing functionality of Lexmark Perspective Document Filters 11.3.0.2400 and 11.4.0.2452. A crafted PDF document can lead to a use-after-free resulting in direct code execution. CVE-2017-2821	NA	A-LEX-PERCE-140817/69
--------------	------------	-----	--	----	-----------------------

Ledger-cli

Ledger

Execute Code	2017-09-05	6.8	An exploitable use-after-free vulnerability exists in the account parsing component of the Ledger-CLI 3.1.1. A specially crafted ledger file can cause a use-after-free vulnerability resulting in arbitrary code execution. An attacker can convince a user to load a journal file to trigger this vulnerability. CVE-2017-2808	NA	A-LED-LEDGE-140817/70
--------------	------------	-----	--	----	-----------------------

Execute Code Overflow	2017-09-05	6.8	An exploitable buffer overflow vulnerability exists in the tag parsing functionality of Ledger-CLI 3.1.1. A specially crafted journal file can cause an integer underflow resulting in code execution. An attacker can construct a malicious journal file to trigger this vulnerability. CVE-2017-2807	NA	A-LED-LEDGE-140817/71
-----------------------	------------	-----	--	----	-----------------------

Libzip Project

Libzip

DoS Overflow	2017-09-01	4.3	The <code>_zip_read_eocd64</code> function in <code>zip_open.c</code> in libzip before 1.3.0 mishandles EOCD records, which allows remote attackers to cause a denial of	NA	A-LIB-LIBZI-140817/72
--------------	------------	-----	--	----	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			service (memory allocation failure in _zip_cdir_grow in zip_dirent.c) via a crafted ZIP archive. CVE-2017-14107		
DoS Overflow	2017-09-01	4.3	The _zip_read_eocd64 function in zip_open.c in libzip before 1.3.0 mishandles EOCD records, which allows remote attackers to cause a denial of service (memory allocation failure in _zip_cdir_grow in zip_dirent.c) via a crafted ZIP archive. CVE-2017-14107	NA	A-LIB-LIBZI-140817/73
Mcafee					
Livesafe					
NA	2017-09-01	4.3	A man-in-the-middle attack vulnerability in the non-certificate-based authentication mechanism in McAfee LiveSafe (MLS) versions prior to 16.0.3 allows network attackers to modify the Windows registry value associated with the McAfee update via the HTTP backend-response. CVE-2017-3898	http://service.mcafee.com/FAQDocument.aspx?lc=1033&id=TS102723	A-MCA-LIVES-140817/74
Livesafe;Security Scan Plus					
Execute Code	2017-09-01	7.5	A Code Injection vulnerability in the non-certificate-based authentication mechanism in McAfee Live Safe versions prior to 16.0.3 and McAfee Security Scan Plus (MSS+) versions prior to 3.11.599.3 allows network attackers to perform a malicious file execution via a HTTP backend-response. CVE-2017-3897	http://service.mcafee.com/FAQDocument.aspx?lc=1033&id=TS102723	A-MCA-LIVES-140817/75

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

Mimedefang					
<i>Mimedefang</i>					
Execute Code	2017-09-01	4.6	MIMEDefang 2.80 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by the init-script.in and mimedefang-init.in scripts. CVE-2017-14102	NA	A-MIM-MIMED-140817/76
Execute Code	2017-09-01	4.6	MIMEDefang 2.80 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by the init-script.in and mimedefang-init.in scripts. CVE-2017-14102	NA	A-MIM-MIMED-140817/77

Mp3gain					
<i>Mp3gain</i>					
Overflow	2017-09-07	4.3	The "mpglibDBL/layer3.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a read access violation when opening a crafted MP3 file. CVE-2017-12912	https://drive.google.com/open?id=0B9DojFnTUSNGeS1hZlJkeGVkYlU	A-MP3-MP3GA-140817/78
Overflow Memory Corruption	2017-09-07	4.3	The "apetag.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a stack memory	https://drive.google.com/open?id=0B9DojFnTUSNGeS1hZlJkeGVkYlU	A-MP3-MP3GA-140817/79

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			corruption when opening a crafted MP3 file. CVE-2017-12911	U	
Overflow	2017-09-07	4.3	The "mpglibDBL/layer3.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a read access violation when opening a crafted MP3 file. CVE-2017-12912	https://drive.google.com/open?id=0B9DojFnTUSNGeS1hZlJkeGVkYlU	A-MP3-MP3GA-140817/80
Overflow Memory Corruption	2017-09-07	4.3	The "apetag.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a stack memory corruption when opening a crafted MP3 file. CVE-2017-12911	https://drive.google.com/open?id=0B9DojFnTUSNGeS1hZlJkeGVkYlU	A-MP3-MP3GA-140817/81

Netapp

Clustered Data Ontap

NA	2017-09-01	4	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to read data on other Storage Virtual Machines (SVMs) via unspecified vectors. CVE-2017-12423	https://kb.netapp.com/support/s/article/NTAP-20170831-0002	A-NET-CLUST-140817/82
Execute Code	2017-09-01	6.5	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to execute arbitrary code on the storage controller via unspecified vectors. CVE-2017-12421	https://kb.netapp.com/support/s/article/NTAP-20170831-0002	A-NET-CLUST-140817/83

Oncommand Unified Manager For Clustered Data Ontap

Gain Information	2017-09-01	5	NetApp OnCommand Unified Manager for Clustered Data ONTAP before 7.2P1 does not set the secure flag for an unspecified cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	https://kb.netapp.com/support/s/article/NTAP-20170831-0001	A-NET-ONCOM-140817/84
------------------	------------	---	---	---	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			CVE-2017-14053		
Clustered Data Ontap					
NA	2017-09-01	4	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to read data on other Storage Virtual Machines (SVMs) via unspecified vectors. CVE-2017-12423	https://kb.netapp.com/support/s/article/NTAP-20170831-0002	A-NET-CLUST-140817/85
Execute Code	2017-09-01	6.5	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to execute arbitrary code on the storage controller via unspecified vectors. CVE-2017-12421	https://kb.netapp.com/support/s/article/NTAP-20170831-0002	A-NET-CLUST-140817/86
Data Ontap					
DoS	2017-09-01	4	NetApp Data ONTAP before 8.2.5 and 8.3.x before 8.3.2P12 allow remote authenticated users to cause a denial of service via vectors related to unsafe user input string handling. CVE-2016-1895	https://kb.netapp.com/support/s/article/NTAP-20170831-0003	A-NET-DATA-140817/87
Openjpeg					
Openjpeg					
DoS Execute Code Overflow	2017-09-06	6.8	A size-validation issue was discovered in opj_j2k_write_sot in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c) or possibly remote code execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-14152.	NA	A-OPE-OPENJ-140817/88

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			CVE-2017-14164		
DoS Execute Code Overflow	2017-09-05	6.8	A mishandled zero case was discovered in opj_j2k_set_cinema_parameters in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c and opj_j2k_write_sot in lib/openjp2/j2k.c) or possibly remote code execution.	NA	A-OPE-OPENJ-140817/89
			CVE-2017-14152		
DoS Execute Code Overflow	2017-09-05	6.8	An off-by-one error was discovered in opj_tcd_code_block_allocate_data in lib/openjp2/tcd.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_mqc_flush in lib/openjp2/mqc.c and opj_t1_encode_cblk in lib/openjp2/t1.c) or possibly remote code execution.	NA	A-OPE-OPENJ-140817/90
			CVE-2017-14151		

Openldap

Openldap

Execute Code	2017-09-05	1.9	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file	http://www.openldap.org/its/index.cgi?findid=8703	A-OPE-OPENL-140817/91
--------------	------------	-----	---	---	-----------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript. CVE-2017-14159		
Opencv					
<i>Opencv</i>					
NA	2017-09-04	4.3	OpenCV (Open Source Computer Vision Library) 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12597. CVE-2017-14136	NA	A-OPE-OPENC-140817/92
Pragyan Cms Project					
<i>Pragyan Cms</i>					
Sql	2017-09-07	7.5	SQL injection vulnerability in Pragyan CMS 3.0. CVE-2015-4627	https://github.com/delta/pragyan/issues/207	A-PRA-PRAGY-140817/93
Pysvn					
<i>Svn-workbench</i>					
Execute Code	2017-09-06	9.3	svn-workbench 1.6.2 and earlier on a system with xeyes installed allows local users to execute arbitrary commands by using the "Command Shell" menu item while in the directory trunk/\$(xeyes). CVE-2015-0853	https://bugzilla.redhat.com/show_bug.cgi?id=1262928	A-PYS-SVN-W-140817/94
Qemu					
<i>Qemu</i>					
DoS	2017-09-01	5	Use-after-free vulnerability in the softee function in slirp/socket.c in QEMU (aka Quick Emulator) allows attackers to cause a denial of service (QEMU instance crash) by leveraging failure to properly clear ifq_so from	https://bugzilla.redhat.com/show_bug.cgi?id=1486400	A-QEM-QEMU-140817/95

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			pending packets. CVE-2017-13711		
Qemu					
DoS	2017-09-01	2.1	QEMU (aka Quick Emulator), when built with the VGA display emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors involving display update. CVE-2017-13672	https://bugzilla.redhat.com/show_bug.cgi?id=1486560	A-QEM-QEMU-140817/96
DoS	2017-09-01	5	Use-after-free vulnerability in the softee function in slirp/socket.c in QEMU (aka Quick Emulator) allows attackers to cause a denial of service (QEMU instance crash) by leveraging failure to properly clear ifq_so from pending packets. CVE-2017-13711	https://bugzilla.redhat.com/show_bug.cgi?id=1486400	A-QEM-QEMU-140817/97
DoS	2017-09-01	2.1	QEMU (aka Quick Emulator), when built with the VGA display emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors involving display update. CVE-2017-13672	https://bugzilla.redhat.com/show_bug.cgi?id=1486560	A-QEM-QEMU-140817/98
Rarlab					
Unrar					
Overflow	2017-09-03	7.5	unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a stack-based buffer over-read in unrarlib.c, related to ExtrFile and stricomp. CVE-2017-14122	NA	A-RAR-UNRAR-140817/99
Unrar					
NA	2017-09-03	6.8	The DecodeNumber function in unrarlib.c in unrar 0.0.1	NA	A-RAR-UNRAR-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			(aka unrar-free or unrar-gpl) suffers from a NULL pointer dereference flaw triggered by a specially crafted RAR archive. CVE-2017-14121		140817/100
Dir. Trav.	2017-09-03	5	unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a directory traversal vulnerability for RAR v2 archives: pathnames of the form ../[filename] are unpacked into the upper directory. CVE-2017-14120	NA	A-RAR-UNRAR-140817/101

Ruby-lang

Ruby

DoS	2017-09-06	5	The URI.decode_www_form_component method in Ruby before 1.9.2-p330 allows remote attackers to cause a denial of service (catastrophic regular expression backtracking, resource consumption, or application crash) via a crafted string. CVE-2014-6438	https://www.ruby-lang.org/en/news/2014/08/19/ruby-1-9-2-p330-released/	A-RUB-RUBY-140817/102
-----	------------	---	---	---	-----------------------

SAP

Netweaver

NA	2017-09-06	7.5	XML External Entity (XXE) vulnerability in SAP Netweaver before 7.01. CVE-2015-7241	NA	A-SAP-NETWE-140817/103
----	------------	-----	--	----	------------------------

Salesagility

Suitecrm

Execute Code	2017-09-06	9.3	Race condition in SuiteCRM before 7.2.3 allows remote attackers to execute arbitrary code. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-5947. CVE-2015-5948	https://github.com/XiphosResearch/exploits/tree/master/suiteshell	A-SAL-SUITE-140817/104
--------------	------------	-----	---	---	------------------------

Sefrengo

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

Sefrengo					
Sql	2017-09-07	7.5	SQL injection vulnerability in Sefrengo before 1.6.5 beta2. CVE-2015-5052	http://forum.sefrengo.org/index.php?showtopic=3399	A-SEF-SEFRE-140817/105
Scrapy					
Scrapy					
DoS	2017-09-05	7.8	Scrapy 1.4 allows remote attackers to cause a denial of service (memory consumption) via large files because arbitrarily many files are read into memory, which is especially problematic if the files are then individually written in a separate thread to a slow storage resource, as demonstrated by interaction between dataReceived (in core/downloader/handlers/http11.py) and S3FilesStore. CVE-2017-14158	NA	A-SCR-SCRAP-140817/106
Simplesamlphp					
Infocard Module					
NA	2017-09-01	5	The InfoCard module 1.0 for SimpleSAMLphp allows attackers to spoof XML messages by leveraging an incorrect check of return values in signature validation utilities. CVE-2017-12874	https://simplesamlphp.org/security/201612-03	A-SIM-INFOC-140817/107
Simplesamlphp					
Gain Information	2017-09-01	7.5	SimpleSAMLphp 1.7.0 through 1.14.10 might allow attackers to obtain sensitive information, gain unauthorized access, or have unspecified other impacts by leveraging incorrect persistent NameID generation when an Identity Provider (IdP) is	https://simplesamlphp.org/security/201612-04	A-SIM-SIMPL-140817/108

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			misconfigured. CVE-2017-12873		
Gain Information	2017-09-01	4.3	The (1) Htpasswd authentication source in the authcrypt module and (2) SimpleSAML_Session class in SimpleSAMLphp 1.14.11 and earlier allow remote attackers to conduct timing side-channel attacks by leveraging use of the standard comparison operator to compare secret material against user input. CVE-2017-12872	https://simplesamlphp.org/security/201703-01	A-SIM-SIMPL-140817/109
Bypass	2017-09-01	4.3	The aesEncrypt method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.x through 1.14.11 makes it easier for context-dependent attackers to bypass the encryption protection mechanism by leveraging use of the first 16 bytes of the secret key as the initialization vector (IV). CVE-2017-12871	https://simplesamlphp.org/security/201703-02	A-SIM-SIMPL-140817/110
Gain Information	2017-09-01	4.3	SimpleSAMLphp 1.14.12 and earlier make it easier for man-in-the-middle attackers to obtain sensitive information by leveraging use of the aesEncrypt and aesDecrypt methods in the SimpleSAML/Utils/Crypto class to protect session identifiers in replies to non-HTTPS service providers. CVE-2017-12870	https://simplesamlphp.org/security/201704-01	A-SIM-SIMPL-140817/111
Bypass	2017-09-01	5	The multiauth module in SimpleSAMLphp 1.14.13 and earlier allows remote attackers to bypass authentication context restrictions and use an	https://simplesamlphp.org/security/201704-02	A-SIM-SIMPL-140817/112

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			authentication source defined in config/authsources.php via vectors related to improper validation of user input. CVE-2017-12869		
Bypass	2017-09-01	7.5	The secureCompare method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.13 and earlier, when used with PHP before 5.6, allows attackers to conduct session fixation attacks or possibly bypass authentication by leveraging missing character conversions before an XOR operation. CVE-2017-12868	https://github.com/simplesamlphp/simplesamlphp/commit/4bc629658e7b7d17c9ac3fe0da7dc5df71f1b85e	A-SIM-SIMPL-140817/113
Infocard Module					
NA	2017-09-01	5	The InfoCard module 1.0 for SimpleSAMLphp allows attackers to spoof XML messages by leveraging an incorrect check of return values in signature validation utilities. CVE-2017-12874	https://simplesamlphp.org/security/201612-03	A-SIM-INFOC-140817/114
Simplesamlphp					
Gain Information	2017-09-01	7.5	SimpleSAMLphp 1.7.0 through 1.14.10 might allow attackers to obtain sensitive information, gain unauthorized access, or have unspecified other impacts by leveraging incorrect persistent NameID generation when an Identity Provider (IdP) is misconfigured. CVE-2017-12873	https://simplesamlphp.org/security/201612-04	A-SIM-SIMPL-140817/115
Gain Information	2017-09-01	4.3	The (1) Htpasswd authentication source in the authcrypt module and (2)	https://simplesamlphp.org/security/201703-01	A-SIM-SIMPL-140817/116

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			SimpleSAML_Session class in SimpleSAMLphp 1.14.11 and earlier allow remote attackers to conduct timing side-channel attacks by leveraging use of the standard comparison operator to compare secret material against user input. CVE-2017-12872		
Bypass	2017-09-01	4.3	The aesEncrypt method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.x through 1.14.11 makes it easier for context-dependent attackers to bypass the encryption protection mechanism by leveraging use of the first 16 bytes of the secret key as the initialization vector (IV). CVE-2017-12871	https://simplesamlphp.org/security/201703-02	A-SIM-SIMPL-140817/117
Gain Information	2017-09-01	4.3	SimpleSAMLphp 1.14.12 and earlier make it easier for man-in-the-middle attackers to obtain sensitive information by leveraging use of the aesEncrypt and aesDecrypt methods in the SimpleSAML/Utils/Crypto class to protect session identifiers in replies to non-HTTPS service providers. CVE-2017-12870	https://simplesamlphp.org/security/201704-01	A-SIM-SIMPL-140817/118
Bypass	2017-09-01	5	The multiauth module in SimpleSAMLphp 1.14.13 and earlier allows remote attackers to bypass authentication context restrictions and use an authentication source defined in config/authsources.php via vectors related to improper validation of user input.	https://simplesamlphp.org/security/201704-02	A-SIM-SIMPL-140817/119

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			CVE-2017-12869		
Bypass	2017-09-01	7.5	The secureCompare method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.13 and earlier, when used with PHP before 5.6, allows attackers to conduct session fixation attacks or possibly bypass authentication by leveraging missing character conversions before an XOR operation. CVE-2017-12868	https://github.com/simplesamlphp/simplesamlphp/commit/4bc629658e7b7d17c9ac3fe0da7dc5df71f1b85e	A-SIM-SIMPL-140817/120
Soreco					
Xpert.line					
Gain Privileges	2017-09-07	7.5	Soreco Xpert.Line 3.0 allows local users to spoof users and consequently gain privileges by intercepting a Windows API call. CVE-2015-3442	NA	A-SOR-XPERT-140817/121
Strongswan					
Strongswan					
DoS Execute Code	2017-09-07	7.5	strongSwan 5.2.2 and 5.3.0 allows remote attackers to cause a denial of service (daemon crash) or execute arbitrary code. CVE-2015-3991	https://bugzilla.redhat.com/show_bug.cgi?id=1222815	A-STR-STRON-140817/122
Suitecrm					
Suitecrm					
Execute Code	2017-09-06	6.8	SuiteCRM before 7.2.3 allows remote attackers to execute arbitrary code. CVE-2015-5947	https://github.com/XiphosResearch/exploits/tree/master/suiteshell	A-SUI-SUITE-140817/123
Sumo					
Google Analyticator					
CSRF	2017-09-07	6.8	Cross-site request forgery (CSRF) vulnerability in Google Analyticator Wordpress Plugin before	NA	A-SUM-GOOGLE-140817/124

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			6.4.9.3 rev @1183563. CVE-2015-4697		
Symantec					
Proxyclient					
Execute Code	2017-09-01	7.2	Symantec ProxyClient 3.4 for Windows is susceptible to a privilege escalation vulnerability. A malicious local Windows user can, under certain circumstances, exploit this vulnerability to escalate their privileges on the system and execute arbitrary code with LocalSystem privileges. CVE-2017-13674	https://www.symantec.com/security-center/network-protection-security-advisories/SA152	A-SYM-PROXY-140817/125
Execute Code	2017-09-01	7.2	Symantec ProxyClient 3.4 for Windows is susceptible to a privilege escalation vulnerability. A malicious local Windows user can, under certain circumstances, exploit this vulnerability to escalate their privileges on the system and execute arbitrary code with LocalSystem privileges. CVE-2017-13674	https://www.symantec.com/security-center/network-protection-security-advisories/SA152	A-SYM-PROXY-140817/126
Synology					
Photo Station					
NA	2017-09-08	4	Server-side request forgery (SSRF) vulnerability in file_upload.php in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allows remote authenticated users to download arbitrary local files via the url parameter. CVE-2017-12071	https://www.synology.com/en-global/support/security/Synology_SA_17_35_PhotoStation	A-SYN-PHOTO-140817/127
Dir. Trav.	2017-09-08	4	Directory traversal vulnerability in synphotoio in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allows remote	https://www.synology.com/en-global/support/security/Synology_SA_17_35_Photo	A-SYN-PHOTO-140817/128

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			authenticated users to read arbitrary files via unspecified vectors. CVE-2017-11162	Station	
Execute Code Sql	2017-09-08	7.5	Multiple SQL injection vulnerabilities in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allow remote attackers to execute arbitrary SQL commands via the (1) article_id parameter to label.php; or (2) type parameter to synotheme.php. CVE-2017-11161	https://www.synology.com/en-global/support/security/Synology_SA_17_35_Photo Station	A-SYN-PHOTO-140817/129
Tune Library Project					
Tune Library					
Sql	2017-09-07	6.8	SQL injection vulnerability in WordPress Tune Library plugin before 1.5.5. CVE-2015-3314	https://wordpress.org/plugins/tune-library/#developers	A-TUN-TUNE - 140817/130
Vulcanjs					
Vulcan					
XSS Gain Information	2017-09-06	5	TelescopeJS before 0.15 leaks user bcrypt password hashes in websocket messages, which might allow remote attackers to obtain password hashes via a cross-site scripting attack. CVE-2015-3454	https://github.com/VulcanJS/Vulcan/commit/827a15dc7422b2447f3a2e395b5e511379002ea4	A-VUL-VULCA-140817/131
Xnau					
Participants Database					
XSS	2017-09-04	4.3	The Participants Database plugin before 1.7.5.10 for WordPress has XSS. CVE-2017-14126	https://wordpress.org/plugins/participants-database/#developers	A-XNA-PARTI-140817/132
Operating System (OS)					
Google					
Android					
NA	2017-09-08	6.8	A elevation of privilege	https://source.a	O-GOO-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			vulnerability in the MediaTek mmc driver. Product: Android. Versions: Android kernel. Android ID: A-36274676. References: M-ALPS03361487. CVE-2017-0804	ndroid.com/security/bulletin/2017-09-01	ANDRO-140817/133
NA	2017-09-08	6.8	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-36136137. References: M-ALPS03361477. CVE-2017-0803	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/134
NA	2017-09-08	6.8	A elevation of privilege vulnerability in the MediaTek kernel. Product: Android. Versions: Android kernel. Android ID: A-36232120. References: M-ALPS03384818. CVE-2017-0802	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/135
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek libmtkomxvdec. Product: Android. Versions: Android kernel. Android ID: A-38447970. References: M-ALPS03337980. CVE-2017-0801	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/136
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek teei. Product: Android. Versions: Android kernel. Android ID: A-37683975. References: M-ALPS03302988. CVE-2017-0800	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/137
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek lastbus. Product: Android. Versions: Android kernel. Android ID: A-	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/138

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			36731602. References: M-ALPS03342072. CVE-2017-0799		
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek kernel. Product: Android. Versions: Android kernel. Android ID: A-36100671. References: M-ALPS03365532. CVE-2017-0798	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/139
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-62459766. References: M-ALPS03353854. CVE-2017-0797	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/140
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek auxadc driver. Product: Android. Versions: Android kernel. Android ID: A-62458865. References: M-ALPS03353884, M-ALPS03353886, M-ALPS03353887. CVE-2017-0796	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/141
NA	2017-09-08	9.3	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-36198473. References: M-ALPS03361480. CVE-2017-0795	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/142
Gain Information	2017-09-08	3.3	A information disclosure vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37305578. References: B-	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/143

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			V2017052301. CVE-2017-0792		
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37306719. References: B-V2017052302. CVE-2017-0791	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/144
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37357704. References: B-V2017053101. CVE-2017-0790	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/145
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37685267. References: B-V2017053102. CVE-2017-0789	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/146
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37722328. References: B-V2017053103. CVE-2017-0788	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/147
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37722970. References: B-V2017053104. CVE-2017-0787	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/148
NA	2017-09-08	5.8	A elevation of privilege vulnerability in the Broadcom wi-fi driver.	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-140817/149

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			Product: Android. Versions: Android kernel. Android ID: A-37351060. References: B-V2017060101. CVE-2017-0786	17-09-01	
IBM					
En6131 Firmware;lb6131 Firmware					
CSRF	2017-09-07	6.8	Cross-site request forgery (CSRF) vulnerability in IBM Flex System EN6131 40Gb Ethernet and IB6131 40Gb Infiniband Switch firmware 3.4.0000 and earlier. CVE-2014-9565	https://support.podc.sl.edst.ibm.com/support/home/docdisplay?lnidocid=MIGR-5098173	O-IBM-EN613-140817/150
Linux					
Linux Kernel					
Gain Information	2017-09-05	2.1	The atyfb_ioctl function in drivers/video/fbdev/aty/atyfb_base.c in the Linux kernel through 4.12.10 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading locations associated with padding bytes. CVE-2017-14156	NA	O-LIN-LINUX-140817/151
Gain Information	2017-09-05	2.1	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR. CVE-2017-14140	https://github.com/torvalds/linux/commit/197e7e521384a23b9e585178f3f11c9fa08274b9	O-LIN-LINUX-140817/152
DoS	2017-09-01	4.9	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system	http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=499350a5a6e7512d9ed369ed63a4244b	O-LIN-LINUX-140817/153

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			crash) by triggering a disconnect within a certain tcp_recvmsg code path. CVE-2017-14106	6536f4f8	
DoS	2017-09-01	4.9	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path. CVE-2017-14106	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=499350a5a6e7512d9ed369ed63a4244b6536f4f8	O-LIN-LINUX-140817/154

Netapp

Data Ontap

Bypass Gain Information	2017-09-01	7.5	NetApp Data ONTAP before 8.2.4, when operating in 7-Mode, allows remote attackers to bypass authentication and (1) obtain sensitive information from or (2) modify volumes via vectors related to UTF-8 in the volume language. CVE-2015-7746	https://kb.netapp.com/support/index?page=content&id=9010049	O-NET-DATA-140817/155
-------------------------	------------	-----	---	---	-----------------------

Paloaltonetworks

Pan-os

XSS	2017-09-07	4.3	Cross-site scripting (XSS) vulnerability in the GlobalProtect internal and external gateway interface in Palo Alto Networks PAN-OS before 6.1.18, 7.0.x before 7.0.17, 7.1.x before 7.1.12, and 8.0.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via vectors related to improper request parameter validation. CVE-2017-12416	http://securityadvisories.paloaltonetworks.com/Home/Detail/93	O-PAL-PAN-O-140817/156
XSS	2017-09-07	4.3	Cross-site scripting (XSS)	http://securityadvisories.paloaltonetworks.com/Home/Detail/93	O-PAL-PAN-O-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

			vulnerability in the GlobalProtect internal and external gateway interface in Palo Alto Networks PAN-OS before 6.1.18, 7.0.x before 7.0.17, 7.1.x before 7.1.12, and 8.0.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via vectors related to improper request parameter validation. CVE-2017-12416	dvisories.paloaltonetworks.com/Home/Detail/93	140817/157
--	--	--	---	---	------------

Technicolor

Td5336 Firmware

Execute Code	2017-09-04	10	Command Injection in the Ping Module in the Web Interface on Technicolor TD5336 OI_Fw_v7 devices allows remote attackers to execute arbitrary OS commands as root via shell metacharacters in the pingAddr parameter to mnt_ping.cgi. CVE-2017-14127	http://jordyf.me/2017/09/02/technicolor-pwn.html	O-TEC-TD533-140817/158
--------------	------------	----	--	---	------------------------

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										